Darrell D. Slone, Director, Counterintelligence
Darrell.d.slone@nasa.gov

Current Terrorist Threat Condition
No Active Alerts

NASA CI/CT MONTHLY NEWS UPDATE – June 2015

This monthly newsletter is published to increase NASA personnel awareness of significant current issues related to counterintelligence, counterterrorism, and counterintelligence cyber matters. To learn more about CI/CT awareness, or to schedule a CI/CT presentation, please contact the CI POC located on the last page.

Significant Counterterrorism (CT) Issues:

ISIS VICTORIES DISPEL HOPE OF A SWIFT DECLINE

In the past two weeks, the Islamic State has proven its resilience once again. Last weekend it solidified its hold on Iraq's Anbar Province with a carefully choreographed assault on the regional capital, Ramadi.
http://www.nytimes.com/2015/05/24/world/middleeast/with-victories-isis-dispels-hope-of-a-swift-decline.html?_r=0

LONE-WOLF TERROR ATTACK COULD COME AT ANY TIME: DHS SECRETARY

A lone-wolf terrorist could attack the United States at any time, Homeland Security Secretary Johnson warned recently.
http://nypost.com/2015/05/11/lone-wolf-terror-attack-could-come-at-any-time-homeland-security-secretary/

Significant Counterintelligence Issues:

WOMAN IN DUPONT ECONOMIC ESPIONAGE CASE PLEADS GUILTY

A woman accused along with her husband and former DuPont engineers of stealing trade secrets and selling them to China, has pleaded guilty to a related charge. Authorities say the woman and her husband paid retired DuPont engineers thousands of dollars for sensitive company documents about how to make a white pigment known as titanium dioxide.
http://www.usnews.com/news/business/articles/2015/05/06/woman-in-dupont-economic-espionage-case-pleads-guilty

CHINESE PROFESSORS AMONG SIX CHARGED WITH ECONOMIC ESPIONAGE

Two Chinese professors, who for years worked as engineers in the U.S., are among six Chinese nationals accused by federal prosecutors of economic espionage. They were sponsored by their home government in the alleged theft of radio frequency filter technology developed by two U.S. companies.
http://www.usatoday.com/story/news/nation/2015/05/19/china-espionage-technology/27570735/

Significant Cyber Issues:

SPEARFISHING: A NEW WEAPON IN CYBER-TERRORISM

Spear phishing and its evolutions like the "watering hole" attack represent one of the most insidious attack techniques adopted by the majority of threat actors in cyber space. According to the experts at Trend Micro security firm, spear phishing is the attack method used in some 91 percent of cyber-attacks.
http://resources.infosecinstitute.com/spearphishing-a-new-weapon-in-cyber-terrorism/

ARE WE EXAGGERATING CHINA'S CYBER THREAT?

So how much should we worry about China's cyber capabilities? Not much, according to a professor's new policy brief, published by Harvard University's Belfer Center. Public record on U.S. and Chinese cyber capabilities remains scant, but the professor suggests that the U.S. is gaining an "increasing advantage," evidenced by a new DARPA program launched in 2012, and the use of the Stuxnet worm against Iran.
http://thediplomat.com/2015/05/are-we-exaggerating-chinas-cyber-threat/

Analyst Notes – Items to Watch:

The reports of the decline of ISIS have turned out to be **extremely** premature. Western indecisiveness and lack of effective military resistance, coupled with recent ISIS offensives have led to significant ISIS successes in both Syria and Iraq. In addition, the widespread use of social media by ISIS has resulted in new recruits flocking to their cause; as well as an increased threat of "lone wolf" attacks against the West, including the United States. Although Al Qaeda (AQ) has not had the "flashy" success of ISIS as of late, AQ continues to have success in Syria through their affiliate Al-Nusra and in Yemen, with battlefield victories as well as expanded membership. Economic espionage against the United States has yielded the Chinese a treasure trove of advanced technology, with some being gathered by agents (old school) and some being stolen via computer networks. The NASA CI/CT division will continue to monitor these threats and any others that emerge in the future that have the potential to harm NASA or its equities.

NASA CI Offices:

Ames Research Center: Christopher Knoth, (650) 604-2250
Armstrong Flight Research Center: Frank Sutton, (661) 276-7476
Glenn Research Center: George Crawford, (216) 433-8458
Goddard Space Flight Center: Christian Breil, (301) 286-1533
Jet Propulsion Laboratory: John J. O'Malley, (818) 354-7828
Johnson Space Center: Tony Dietsch, (281) 483-7921
Kennedy Space Center: Ron Storey, (321) 867-2568
Langley Research Center: Benjamin Marchione, (757) 864-3403
Marshall Space Flight Center: Brian Tindall, (256) 544-4095
NASA Headquarters: Art Payton, (202) 358-4645
Stennis Space Center: David Malcom, (228) 688-1683